**Jason K. Singleton, State Bar #166170**
**jason@singletonlawgroup.com**
**Richard E. Grabowski, State Bar #236207**
**rgrabowski@mckinleyville.net**
**SINGLETON LAW GROUP**
**611 "L" Street, Suite A**
**Eureka, CA 95501**

**(707) 441-1177**
**FAX 441-1533**

**Attorneys for Plaintiff, ASIS INTERNET SERVICES**

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

| | |
|---|---|
| **ASIS INTERNET SERVICES, a California corporation**<br><br>**Plaintiff,**<br>**vs.**<br><br>**MEMBER SOURCE MEDIA, LLC, a California limited liability company, et al.,**<br><br>**Defendants.** | **Case No. C-08-1321 EMC**<br><br>**PLAINTIFF'S REPLY TO DEFENDANT 'S OPPOSITION TO MOTION TO SEAL**<br><br>**DATE: September 3, 2008**<br>**TIME: 10:30 a.m.**<br>**CTRM: C, 15th floor** |

**Plaintiff, ASIS INTERNET SERVICES,** herein replies to Defendant Member Source Media's Opposition to File Certain Documents under Seal..

Defendant asserts that the items requested sealed by Plaintiff do not meet the requirements for sealing as required by LR 79.5.

The documents requested sealed by Plaintiff are the actual emails sent to Plaintiff by Defendant's affiliates. These emails contain email accounts owned by Plaintiff ASIS. These emails are the corporate property of ASIS. Defendant is well aware of what is contained in these files and the sensitive nature of Plaintiff's email accounts. Unlike as asserted by Defendant, ASIS has never exposed its email addresses to public exposure and Defendant provides no evidence that these email addresses have ever been exposed. If Defendant has any such evidence then it should present it so that Plaintiff can begin prosecution of the offending parties. If Defendant has exposed Plaintiff's email accounts to bulk email

processors, then Defendant has done so in direct violation of the Protective Order in this case. Plaintiff has always requested that its email addresses be kept confidential.

Plaintiff requests that its email addresses be kept confidential because of the exposure to injury from spammers and hackers. Hackers regularly attempt to illegally penetrate ISP's directory servers with the intent of stealing email address lists to sell to spammers. Exposing this list of emails to the public would subject Plaintiff to even more SPAM attacks than it currently endures. In addition, most of the email addresses belonged to actual consumers at one time. Those consumers have the ability to re-activate those accounts. They would then be subject to increased spam attacks. In addition, a portion of the email addresses are internal administrative accounts used by ASIS to run its business. Exposure of these addresses would lead to a significant increase of SPAM, and since these are administrative accounts may also lead to security breaches on Plaintiff's servers.

Defendant's aspersions that Plaintiff wishes to receive more SPAM in order to bring SPAM suits is ridiculous. Neither Plaintiff nor any other ISP needs to do anything to get more SPAM. Plaintiff receives approximately 200,000 SPAM emails per day. Large ISPs such as Microsoft or AOL receive over a billion emails a day. Every ISP, including Plaintiff, must pay continuously to filter and process these SPAM emails. The estimated cost for processing SPAM is $198 billion per year worldwide. The Internet Direct Marketing industry (SPAMMERs) generates about $2 billion per year in revenue. This means that the public pays $198 billion per year so the SPAMMERS can walk away with $2 billion. This is why the legislature created the ***CAN SPAM ACT*** and created a private attorney general action by ISPs. That is why Plaintiff is bringing suits in order to stop spamming by both injunction and statutory penalties. This is the purpose of the ***CAN SPAM Act of 2003*** and the reason the legislature provided standing to ISPs. Defendant is a well known spammer with multiple judgments for spamming. Plaintiff is asserting its rights as established under the ***CAN SPAM Act of 2003*** in prosecuting a case against a known spammer who has misused Plaintiff's resources to send garbage to Plaintiff's customers and Plaintiff's servers. It is not true that these SPAM emails only went to inactive accounts, they also went to live consumer accounts. However, because Plaintiff is

adamant about protecting its customers it will not jeopardize their safety by involving them in lawsuits against SPAMMERS.

Plaintiff delivered the SPAM emails with Plaintiff's un-redacted email accounts as proof that Plaintiff had received the emails. Because of the volume of the emails, 5006 for MSM and 214 for Vantage, Plaintiff has to deliver the emails electronically on CD. The electronic form used allows the Court to view the emails in an email browser without actually loading the emails on its computer, thus avoiding the problems with viruses and worms prevalent in SPAM. Therefore, while Plaintiff is only designating its email accounts as confidential, it is impossible to produce the data in a manner that the Court can use without designating the entire file confidential. If the Court requires, Plaintiff can produce a set of emails, not under seal, with Plaintiff's email accounts redacted. However, in this form the emails will not demonstrate that they were sent to "asis.com" email addresses.

Defendant's motives in making this claim are suspect, as Defendant's counsel have always attempted to expose Plaintiff's corporate information in an attempt to force Plaintiff to withdraw. The Court should not support the efforts of a known spammer to expose Plaintiff's protected information.

**SINGLETON LAW GROUP**

Dated: August 21, 2008

/s/ Jason K. Singleton
Jason K. Singleton
Richard E. Grabowski, Attorneys for Plaintiff,
**ASIS INTERNET SERVICES**